AMENDMENTS TO THE CLAIMS

1. (Original) A method, comprising:

parsing a data stream to find a predefined synchronization point within the data stream; and

placing non-compliant data near the synchronization point in the data stream;

wherein the data stream is decodable by a compliant decoder, after the non-compliant data is replaced with compliant data.

2. (Original) The method as recited in claim 1, further comprising:

encrypting a portion of the data stream; and transmitting the portion of the data stream.

3. (Original) The method as recited in claim 2, further comprising:

decrypting the portion of the data stream.

4. (Original) The method as recited in claim 3, wherein the non-compliant data is key information that is used in encrypting and decrypting.

5. (Currently Amended) A method, comprising:

receiving a portion of a data stream;

parsing the portion of the data stream to find a synchronization point within the data stream;

retrieving non-compliant data near the synchronization point;

replacing non-compliant data in the data stream; and

decrypting the portion of the data stream.

6. (Original) The method as recited in claim 5, wherein the non-compliant data is key information that is used in decrypting.

7. (Original) The method as recited in claim 5, further comprising:

replacing the non-compliant data near the synchronization point with compliant data; and decoding the portion of the data stream.

8. (Original) A system, comprising:

an authoring device to use key information to encrypt a portion of a data stream; and

a consumption device in communication with the authoring device, the consumption device to use the key information to decrypt the portion of the data stream.

9. (Original) The system as recited in claim 8, further comprising:

a decoding device in communication with the consumption device to decode the portion of the data stream.

10. (Original) The system as recited in claim 8, wherein the consumption device is configured to retrieve the key information from the portion of the data stream.

11. (Original) A system, comprising:

an authoring device to create a data stream;

an encryption tool to embed key information near each synchronization point in the data stream and to encrypt a portion of the data stream associated with each synchronization point; and

a consumption device to retrieve key information near each synchronization point in the data stream and to replace the key information with compliant data and to use the key information to decrypt the data stream.

12. (Original) The system as recited in claim 11, further comprising:

a decoding device to decode the data stream.

13. (Original) The system as recited in claim 11, further comprising:

a decryption tool to use the key information to decrypt the portion.

14. (Original) A machine-accessible medium having associated content capable of directing the machine to perform a method, the method comprising:

parsing a first data stream to find a packetized elementary stream (PES) header, the PES header associated with at least some payload data;

copying the first data stream to a second data stream; and

selectively inserting compliant data into the second data stream after the PES header, to hold key information associated with the PES header.

15. (Original) The machine-accessible medium as recited in claim 14, wherein the method further comprises:

storing the first data stream; and

storing the second data stream.

16. (Original) The machine-accessible medium as recited in claim 14, wherein the method further comprises:

parsing the second data stream to find each PES header;

embedding key information into each portion of the second data stream after each PES header; and

encrypting each portion of the second data stream.

17. (Original) The machine-accessible medium as recited in claim 16, wherein the method further comprises:

transmitting each portion of the second data stream.

18. (Original) The machine-accessible medium as recited in claim 16, wherein the method further comprises:

retrieving key information from a portion of the second data stream;

decrypting the portion of the second data stream with the key information; and

replacing the key information with compliant data in the portion of the second data stream.

19. (Original) The machine-accessible medium as recited in claim 18, wherein the method further comprises:

decoding the portion.

20. (Currently Amended) A data structure, comprising:

a header;

key information separate from and associated with the header for use in decryption; and

a payload associated with the header, the payload capable of being encrypted using the key information.

21. (Original) The data structure as recited in claim 20, wherein compliant data replaces the key information associated with the header, before decryption.

22. (Original) The data structure as recited in claim 21, wherein the header, compliant data, and decrypted payload are capable of being decoded by a compliant decoder.

23. (Original) The data structure as recited in claim 20, wherein the key information in the header replaces compliant data, after encryption.

24. (Original) The data structure as recited in claim 20, wherein the header is a packetized elementary stream (PES) header and the payload is a PES payload.

25. (Original) A data stream stored on a machine-readable medium, the data stream comprising at least one data structure as recited in claim 20.